UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/663,891	09/18/2000	Robert Chojnacki	N0064US	4137

37583 7590 08/20/2007

NAVTEQ NORTH AMERICA, LLC
222 MERCHANDISE MART
SUITE 900, PATENT DEPT.
CHICAGO, IL 60654

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/663,891	CHOJNACKI, ROBERT	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6 and 8-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6, & 8-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 5 and 7 have been cancelled. Applicant's arguments/amendments with respect to amended claims 1, 8, 10, & 24 and previously presented claims 2-4, 6, 9, 11-23, & 25-39 filed 5/31/2007 have been fully considered and therefore the claims are rejected under new grounds.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3-4, and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and further in view of McMullan Jr. et al., US Patent No. 5,654746 and Shear et al., US Pub. No. 2001/0042043.

As per claim 1:

Chan substantially teaches a method for on-line mass distribution of data products to end users, the method comprising: maintaining a first portion of each of said data products at a first location (col. 10, lines 52-67 and col. 11, lines 9-11), maintaining an unencrypted second portion of each of said data products at a second location, wherein the second location is different from said first location (col. 10, lines 52-67 and col. 11, lines 1-2); for each of said end users, confirming the end user's entitlement to one of said data products (col. 11, lines 11-13); obtaining an unencrypted second portion of said one of said data products from said second

location (col. 11, lines 1-5); after said step of confirming, obtaining an encrypted first portion of said one of said data products at said second location from said first location, obtaining a decryption key and using said decryption key to decrypt said encrypted first portion (col. 11, lines 9-20); combining said decrypted first portion of said one of said data products and said unencrypted second portion of said one of said data products, wherein said step of combining is performed at said second location, wherein said end user is located at said second location (col. 11, lines 39-45), and providing said combined first portion and second portion to said user, wherein the first portion of said data product comprises critical data that enables a program executed on a computing platform to use said data product including both the first portion and the second portion together for an intended purpose (col. 11, lines 39-45).

Not explicitly disclosed is wherein the first portion is stored/maintained in an encrypted form on the central server. However, McMullan Jr. et al. teach control information of digital data is maintained in encrypted form at a server archive in order maintain the data's confidentiality. Furthermore, storing/maintaining critical data in an encrypted form is and has been very well known in the art for quite some time now. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan to maintain/store the first portion of data at the first location in encrypted form as well. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since McMullan Jr. et al. suggest that it is well known to protect data that is stored by encrypting the data before storing in col. 2, lines 8-18 and col. 8, lines 26-40.

Also not explicitly disclosed is storing said combined product on a portable computer-readable storage medium, where said user accesses said combined product from said storage medium with said computer platform at a third location different from said first location and said second location. However, Shear et al. teach that the content may be combined and stored on a disk (e.g. DVD or CD) where the disk maintains control information indicating the user's entitlement rights as assessed prior to allowing the downloading step (par. 283). Furthermore, Shear et al. teach that the disk contents may be accessed via a computing platform which can communicate with another entity to continuously ensure that the entitlement rights are not being exceeded (par. 279). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be stored on a portable medium different from the locations that the data product is combined/downloaded at. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shear et al. suggest that having the control information on the disk in addition to a secure node enables continuous observation that users are not exceeding the rights granted in the entitlement rights for that particular user/data product in 279.

As per claim 3:

Chan and McMullan Jr. et al. substantially teach the method of claim 1. Furthermore, Chan teaches wherein said data products include digital copies of movies (col. 10, lines 52-55).

As per claim 4:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method of claim 1. Furthermore, McMullan Jr. et al. teach wherein said data products include digital copies of musical songs (col. 3, lines 49-58).

As per claim 6:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method, as applied to claim l above. Chan teaches the method further comprising the step of prior to the step of combining, encrypting said first portion of one of said data products (col. 4, lines 25-33).

III. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and McMullan Jr. et al., US Patent No. 5,654746 and Shear et al., US Pub. No. 2001/0042043 as applied to claim 1 above, and further in view of Porter et al., United States Patent No. 5,845,067

As per claim 2:

Chan, McMullan Jr. et al., and Shear et al. substantially teach the method, as applied to claim 1 above. Not explicitly disclosed is the method, wherein said data products include geographic databases. However, Porter et al. teaches that a document can be any information stored as files in a file system, which can equate to the information contained by a geographic database. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan et al. for the data product to include files of geographical information stored in a file system, which is equivalent to a database. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Porter et al. in col. 7, lines 26-32.

IV. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and further in view of Shear et al., US Pub. No. 2001/0042043.

As per claim 8:

Chan teaches a system for secure on-line mass distribution of data products to end users comprising: an authorization server at a first location having associated therewith copies of first portions of a plurality of data products, wherein said first portions of the data products do not include information to enable encrypted data to be decrypted (col. 11, lines 11-13); a plurality of data distribution terminals at a plurality of locations different from said first location, each of said data distribution terminals has stored thereon copies of second portions of said plurality of data products (col. 10, line 52 – col. 11, line 4); a communications system that provides for exchange of data between the entity and said plurality of data distribution terminals (col. 11, lines 7-9), and a data distribution program that provides copies of said data products to those end users who are entitled to have said copies thereof (col. 11, lines 7-11); wherein said data distribution program provides a copy of a data product by combining a copy of the first portion of said data product obtained from said authorization server with a copy of the second portion of said data product obtained from one of said plurality of data distribution terminals, wherein said step of combining is performed at a location of said one of said plurality of data distribution terminals and said end user is located at said location of said one of said plurality of data distribution terminals (col. 11, lines 39-45) .

Not explicitly disclosed is a storing device interface associated with said data distribution terminal, wherein said storage device interface stores said combined product on a portable computer-readable storage medium, wherein said user accesses said combined product from said

storage medium with a computer platform at a location different from said location of said data distribution terminal. However, Shear et al. teach that the content may be combined and stored on a disk (e.g. DVD or CD) where the disk maintains control information indicating the user's entitlement rights as assessed prior to allowing the downloading step (par. 283). Furthermore, Shear et al. teach that the disk contents may be accessed via a computing platform which can communicate with another entity to continuously ensure that the entitlement rights are not being exceeded (par. 279). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be stored on a portable medium different from the locations that the data product is combined/downloaded at. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shear et al. suggest that having the control information on the disk in addition to a secure node enables continuous observation that users are not exceeding the rights granted in the entitlement rights for that particular user/data product in 279.

As per claim 9:

Chan and Shear et al. substantially teach the system, as applied to claim 8 above. Furthermore, Chan teaches wherein said authorization server also has associated therewith an authorization database containing data indicating entitlement by said end users to copies of said data products (col. 10, lines 24-45).

V. Claims 10-22, and 24-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860 and further in view of Ginter et al., United States Patent No. 6,237,786 and Shear et al., US Pub. No. 2001/0042043.

As per claims 10 and 24:

Chan substantially teaches a system/method comprising, in combination: a first entity maintaining the first portion of the data product at a first location (col. 10, lines 52-67); a second entity maintaining the second portion of the data product at a second location different from said first location (col. 11, lines 11-15); a first set of logic executable by the first entity to encrypt the first portion so as to produce an encrypted first portion that can be decrypted using a first decryption key, wherein the first entity sends the encrypted first portion via a telecommunications link to the second entity (col. 11, lines 9-20); a second set of logic executable by the second entity, upon receipt of the encrypted first portion, to record onto the storage medium the encrypted first portion and the second portion wherein an end user of the data product is location at said second location where the encrypted first potion and the second portion are recorded onto the storage medium (col. 11, lines 11-20); and wherein the first portion of said data product comprises critical data that enables a program executed on a computing platform to use said data product including both the first portion and the second portion together for an intended purpose (col. 11, lines 39-45).

Not explicitly disclosed is the third entity gaining access to the first decryption key in order to access the data product. However, Ginter et al. teach that in order for a third party, or any party for that matter, to gain access to the data product they must first have the appropriate decryption key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for a third entity to gain access to the first decryption key in order to access the data product. This modification would have been

obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ginter et al. in col. 131, lines 18-44.

Also not explicitly disclosed is wherein said user accesses said data product at a location different from said first location and said second location. However, Shear et al. teach that the content may be combined and stored on a disk (e.g. DVD or CD) where the disk maintains control information indicating the user's entitlement rights as assessed prior to allowing the downloading step (par. 283). Furthermore, Shear et al. teach that the disk contents may be accessed via a computing platform which can communicate with another entity to continuously ensure that the entitlement rights are not being exceeded (par. 279). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the data product to be stored on a portable medium different from the locations that the data product is combined/downloaded at. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Shear et al. suggest that having the control information on the disk in addition to a secure node enables continuous observation that users are not exceeding the rights granted in the entitlement rights for that particular user/data product in 279. As per claims 11 and 25:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 10 and 24. Furthermore, Ginter et al. teach the method/system wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product, and wherein the second set of logic

is further executable to record onto the storage medium the encrypted authorization key (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claims 12 and 26:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 11 and 25. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-45).

As per claims 13 and 27:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 12 and 26. Furthermore, Ginter et al. teach the method/system wherein the environmental parameter comprises an identification code associated with the entity authorized to access the data product (col. 22, lines 13-45).

As per claims 14 and 28:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 11 and 27. Furthermore, Ginter et al. teach the method/system wherein the third entity generating the second decryption key as the function of the identification code; the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information to validate storage of the data product (col. 131, lines 18-44).

As per claims 15 and 29:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 11 and 25. Furthermore, Ginter et al. teach the method/system wherein a third set of logic executable by a third entity to decrypt the encrypted authorization information, to thereby gain

access to verification information, and to compare at least a portion of the verification information to predetermined information associated with the third entity so as to determine whether the third entity is authorized to gain access to the data product (col. 131, lines 18-67).

As per claims 16 and 31:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 15 and 30. Furthermore, Ginter et al. teach the method/system wherein the predetermined information associated with the third entity comprises an identification code (col. 131, lines 40-44).

As per claims 17 and 30:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 10 and 29. Furthermore, Ginter et al. teach the method/system wherein the first entity sends to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to access the data product (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claims 18 and 33:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 17 and 32. Furthermore, Ginter et al. teach the method/system wherein the second decryption key is derived as a function of an environmental parameter (col. 22, lines 13-25).

As per claims 19 and 34:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 18 and 33. Furthermore, Ginter et al. teach the method/system wherein the environmental

parameter comprises an identification code associated with the entity authorized to store the data product (col. 22, lines 13-25).

As per claims 20 and 35:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 11 and 34. Furthermore, Ginter et al. teach the method/system wherein the third entity generating the second decryption key as the function of the identification code; the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information to validate storage of the data product (col. 104, line 25 – col. 106, line 15).

As per claims 21 and 37:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 11 and 36. Furthermore, Ginter et al. teach the method/system wherein a third set of logic executable by a third entity to decrypt the encrypted authorization information, to thereby gain access to verification information, and to compare at least a portion of the verification information to predetermined information associated with the storage medium so as to determine whether the storage medium is authorized to gain access to store the data product (col. 78, lines 8-58).

As per claims 22 and 38:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 21 and 37. Furthermore, Ginter et al. teach the method/system wherein the predetermined information associated with the storage medium comprises and identification code (col. 22, lines 13-45).

As per claim 32:

Chan, Ginter et al., and Shear et al. substantially teach the method as applied to claim 24. Furthermore, Ginter et al. teach the method further comprising sending to the second entity, together with the encrypted first portion, an encrypted authorization key that can be decrypted using a second decryption key so as to reveal verification information indicative of an entity authorized to store the data product (col. 14, lines 21-43 and col. 22, lines 13-45).

As per claim 36:

Chan, Ginter et al., and Shear et al. substantially teach the method as applied to claim 32. Furthermore, Ginter et al. teach the method further comprising the third entity using the second decryption key to decrypt the encrypted authorization key and to thereby gain access to the verification information; and the third entity using the verification information tot validate storage of the data product (col. 104, line 25 – col. 106, line 15).

VI. Claims 23 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, US Patent No. 6,473,860; Ginter et al., United States Patent No. 6,237,786; and Shear et al., US Pub. No. 2001/0042043as applied to claims 10 and 24 above, and further in view of Ahrens et al., United States Patent No. 5,951,620.

As per claims 23 and 39:

Chan, Ginter et al., and Shear et al. substantially teach the method/system as applied to claims 10 and 24. Not explicitly disclosed is the method/system wherein the third entity comprises a navigation system. However, Ahrens et al. teach the use of a navigation system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chan for the third entity to be a navigation system. This

modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ahrens et al. in col. 7, lines 29-44.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,308,179
2. US Patent No. 5,917,908
3. US Patent No. 6,204,774
4. US Patent No. 6,297,891
5. US Patent No. 6,615,349
6. US Pub. No. 2001/0032088
7. US Pub. No. 2004/0039741

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Nadia Khoshnoodi
Examiner
Art Unit 2137
8/15/2007

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER